Presentation of Recommendations from the

IT Acquisition Management Transformation Rapid Improvement Team (RIT) Pilot Report

Blueprint for Establishing Risk-based Governance of IT Investments in a Net-centric Department of Defense

Presented to:
COTS IT Acquisition Barrier WG
2005 QDR

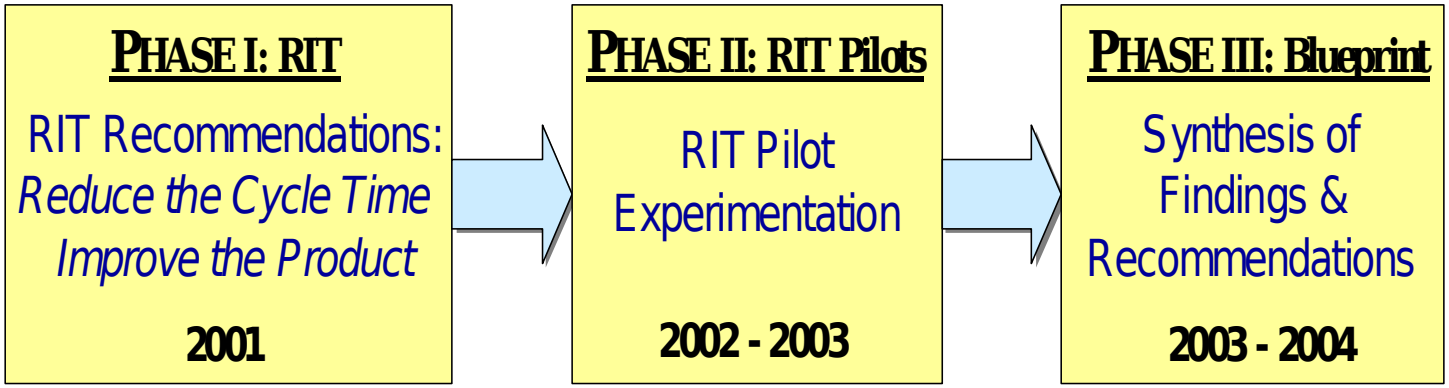
Purpose

- Present recommendations of the IT Acquisition Management Transformation Rapid Improvement Team (RIT) Pilot
- Determine if the recommendations are appropriate for the 2005 QDR IT Working Group or should be referred to another QDR IPT

Issue and Recommendations

- **It takes too long to implement IT solutions needed by the warfighters. How can we shorten the time?**
  - Restructure the PPBE process to finance IT solutions through working capital funds and avoid the current POM process
  - Enable self-organization of the IT/NSS investment community
  - Institute Risk-based Governance

RIT Pilot Summary



Restructure the PPBE process to finance IT solutions through working capital funds

- Recommended by the RIT but not employed by the pilot programs because each had already gone through the POM process
- Comptroller agreed to take for action
- Remains unresolved

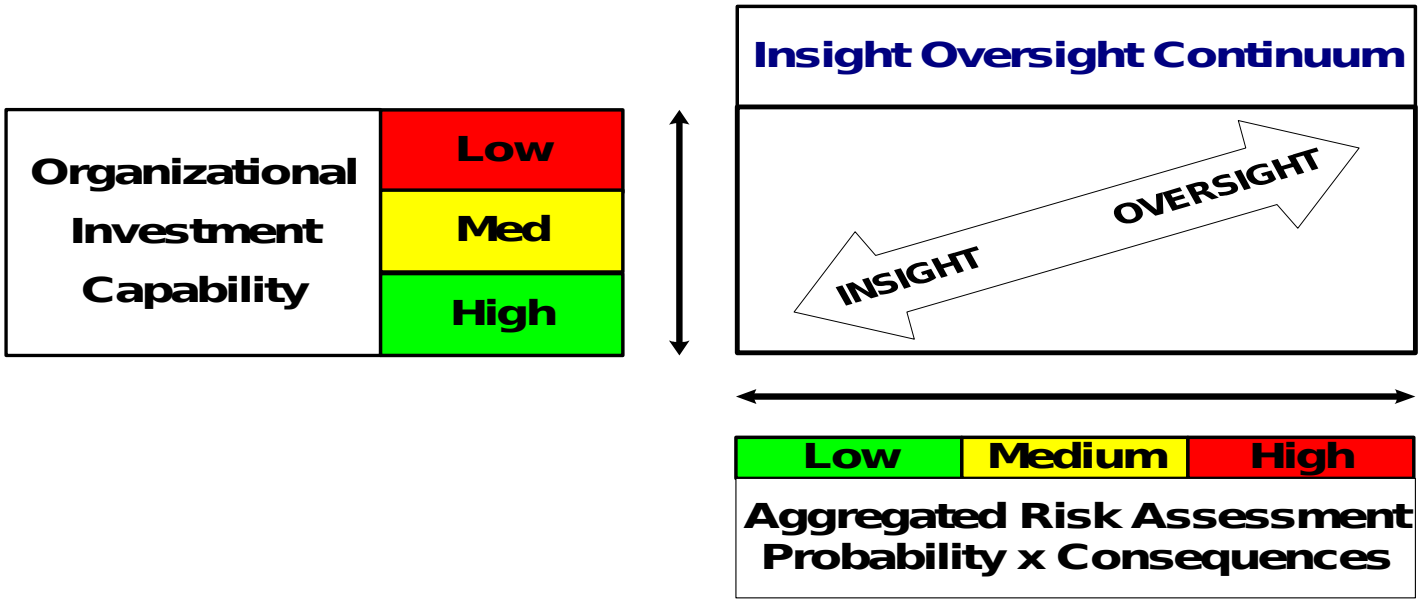
Enable self-organization of the IT investment community

- **What is self organization?**
  - Originated from observation of biological systems
  - Just as the warfighters' exploitation of net-centricity achieved information superiority and in turn enabled self-synchronization, exploitation of net-centricity by the business community can achieve business information superiority and enable self-organization.
- **Why does the business community need self-organization?**
  - US industry leaders are already exploiting self-organization to maintain agility in a global marketplace
  - Since 9-11, the Department has not adequately met the warfighter's need for information superiority.
  - GAO Comptroller General gives warfighter support poor grades
- **Can self-organization work in DoD?**
  - Observed in high performance IT investment organizations such as GCSS-AF and GCSS CC/JTF
  - DoD Data Strategy Communities of Interest (COI) is an example

Institute Risk-based Governance

- **What is Risk-based Governance?**
  - It is the extension of the current 5000.1 policy that states:
    - Responsibility for the acquisition of systems shall be decentralized to the maximum extent practicable, ***consistent with the risk of the investment and the capability of the investing organization to manage the risk.***
- **How is Risk-based Governance different from delegation?**
  - The covenant between the Sponsor, the Acquiring Agency headquarters and the subordinate acquiring echelon is that the delegation of milestone decision authority to the subordinate echelon will add no unacceptable risk to the investment.
  - Enables fast track initiation of IT solutions to warfighter needs
- **What are the prerequisites for Risk-based Governance?**
  - The same as for self-organization

Model of Risk-based Oversight



The hypothesis for the Insight element of RBG is:
Headquarters staff due diligence can be accomplished through timely and transparent insight into JCIDS & PMO work products.

Basis for Risk-based Governance

- **Observation of high performance RIT Pilots revealed five common traits:**
  - Full awareness of the program's objectives within all levels of the Sponsor, PEO and PMO organizations
  - A thorough understanding of the ultimate users' (changing) needs
  - Direct communications with the ultimate users and user surrogates
  - A leadership climate that valued innovation and aggressive management
  - Maximum employment of available net-centric management tools
- **Compares with Alberts and Hayes assumptions for self-synchronization**
  - Clear and consistent understanding of command intent
  - High quality information and shared situational awareness
  - Competence at all levels of the force
  - Trust in the information, subordinates, superiors, peers, and equipment

Attributes of Risk-based Governance

Correlating the RIT Pilot observations with Alberts' self-synchronization assumptions leads to six attributes essential for creating a self-organizing environment we call Risk-based Governance**:**

1. A clear understanding of desired investment outcomes
2. Institutionalized risk assessment and management
3. A collaborative environment with provision for insight into selected investment information sets
4. Process for assessing organizational investment capability
5. Organizational support for capability improvement
6. A trusting relationship between corresponding headquarters and subordinate oversight actors

Recommendations for consideration by the QDR IT Working Group for achieving the six attributes of Risk-based Governance and Self-organization

General Recommendations

1. Change DODD 5000.1 paragraph 4.3.5. Streamlined and Effective Management.

- **From,**
  - "Responsibility for the acquisition of systems shall be decentralized to the maximum extent practicable."
- **To,**
  - "***Responsibility for the investment in systems shall be decentralized to the maximum extent practicable, consistent with the risk of the investment and the capability of the investing organization to manage the risk."***

General Recommendations (con't)

2. **Legislative recommendation:**

   Propose that Congress change the definition of a major program from solely a cost threshold basis to one that includes both cost and the risk of achieving a needed capability or transformation.

A clear understanding of desired investment outcomes

1. That the instruction governing warfighter functional capability boards, CJCSI 3170.01 and CJCSI 3137.01, include as part of FCB responsibilities the articulation of outcome measures of effectiveness as exit criteria for a functional needs analysis, and a commitment to conduct a post implementation review against those measures at appropriate points after the system is fielded.

2. That the portfolio management directives and instructions now being developed by OASD(NII) include provisions for Business Domain Owners to conduct functional area, needs and solutions analyses such as required by CJCSI 3170.01, and that those analyses result in the establishment of outcome measures of effectiveness and the commitment to conduct post implementation reviews against those measures

A clear understanding of desired investment outcomes (cont)

3. That the DoD Enterprise Architecture Performance Reference Model include a process for developing measures of effectiveness (MOEs) and a requirement for an assessment of the MOEs after implementation in a post implementation review (PIR).

Institutionalized Risk Assessment and Management

1. OSD implement risk-based governance and resource an OSD organization to assess OSD and Component IT investment capability.

2. Adopt a generic set of IT acquisition project risk factors, such as is currently being piloted by the US Army, or as has been adopted by the State of Texas Department of Information Resources. Such an inventory of risk factors would be initiated during the Functional Solution Analysis phase and updated as the program evolved

3. Require, as part of Milestone and Decision Reviews, a uniform presentation of investment risk assessment and management using the probability-consequence display format of the DAU Risk Guide

Institutionalized Risk Assessment and Management (cont)

4. Update the DoD Chief Information Officer October 24, 2001 Memorandum, Subject: Policy and Procedures for the Fast Track Deployment of Information Technology, to reflect Risk-based Governance, and urgent program initiation

5. Charter an IPT of OSD and JS gatekeepers and Component representatives to reach agreement about the minimum content and approval process for consolidated acquisition information for Fast Track IT programs

A collaborative environment with provision for insight into selected investment information sets

The hypothesis for the Insight element of RBG is:

- ***Headquarters staff due diligence can be accomplished through timely and transparent insight into JCIDS & PMO work products.***

1. Form an IT investment COI that includes JS, OSD and Component investment actors and exploits NCES
2. Charter an IPT to identify investment information objects needed to conduct insight in a Net-centric investment environment and develop a plan for implementation
3. Identify NCES compatible applications to provide the desired investment insight

Process for Assessing Organizational Investment Capability

1. Integrate RBG capability assessment appraisals with the requirement of the FY 03 National Defense Authorization Act for the Defense Services and specified Agencies to establish Software Acquisition Process Improvement Programs and associated assessments
2. Validate and adopt the Software Engineering Institute CMMI-AM be as the standard IT acquisition capability assessment model for PEO and PM organizations.
3. Each OSD investment gatekeeper develop a process for appraising their Component counterpart organizational capability

Organizational Support for Capability Improvement

1. Adopt a proactive posture for quality management that includes continuous capability improvement throughout the Department and articulate it within the directive system
2. Identify the Quality Management Office within the Office of the Secretary of Defense to serve as the focal point for investment performance excellence
3. Establish a Quality Management Community of Practice

Engender a Trusting Relationship Between Corresponding OSD, JS and Component IT Investment Gatekeepers

1. Implementation of the preceding recommendations supports a ***trust but verify*** relationship amongst gatekeeper counterparts
   - The culture of the Department is one of information hoarding rather than sharing.
   - Changes in the JCIDS and Acquisition processes that enable decentralization of responsibility engender trust
   - The RIT Pilot undertook a trust building exercise with capability assessments that resulted in broad publication of the reports
   - Transformation to a net-centric data sharing environment creates transparency that engenders trust
   - Component portals are providing investment decision and progress transparency

The full report of the

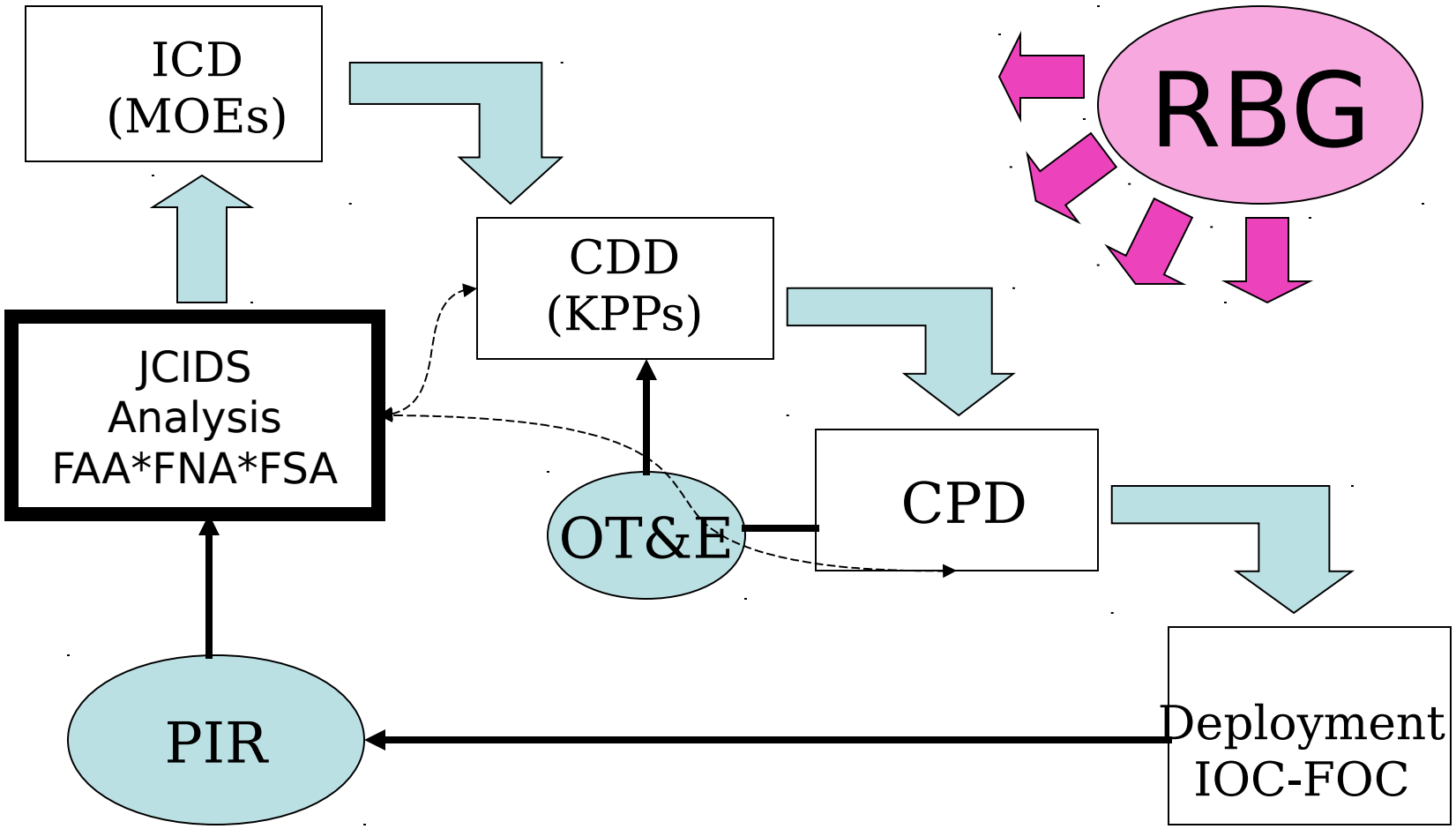
IT Acquisition Management Transformation Rapid Improvement Team (RIT) Pilot Report

Blueprint for Establishing Risk-based Governance of IT Investments in a Net-centric Department of Defense

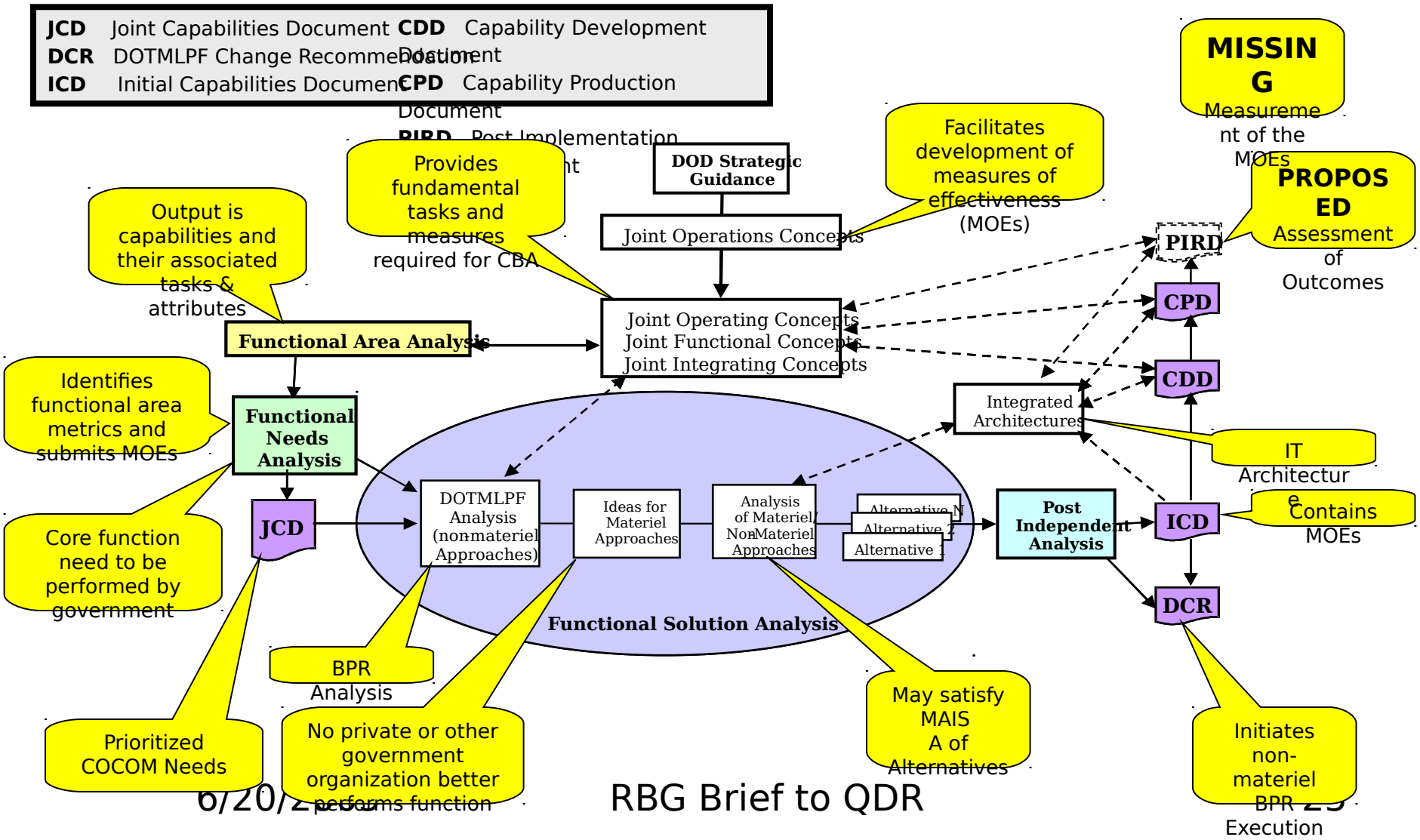
is available electronically in the
IT Community of Practice
at URL:
https://acc.dau.mil/simplify/ev.php?ID=16223_201&ID2=DO_TOPIC

BACK UP

Making Fast Track Feasible by Calibrating RBG with Outcomes



Existing and Proposed JCIDS Processes for Satisfying CCA



Post Implementation Review (PIR) in the JCIDS ICD Life Cycle